#13 AL

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平10－257048

(43)公開日　平成10年(1998) 9月25日

(51)Int.Cl.[6]	識別記号	FI	
H04L 9/32		H04L 9/00	673A
G06F 15/00	330	G06F 15/00	330B

審査請求　未請求　請求項の数20　ＯＬ　（全 15 頁）

(21)出願番号　特願平10－4566

(22)出願日　平成10年(1998) 1月13日

(31)優先権主張番号　08／790041

(32)優先日　1997年1月28日

(33)優先権主張国　米国（US）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州アーモンク　（番地なし）

(72)発明者　シャウーペン・シ
アメリカ合衆国78726、テキサス州オースティン、エリカ・レイ・コート　10502

(74)代理人　弁理士　坂口　博　（外１名）

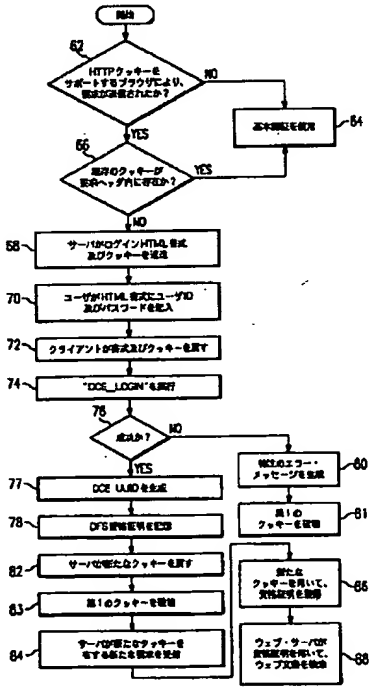
最終頁に続く

(54)【発明の名称】　クッキーによる分散ファイル・システム・ウェブ・サーバ・ユーザの認証

(57)【要約】　（修正有）

【課題】　分散コンピュータ環境の分散ファイル・システムに接続可能なウェブ・サーバに、ウェブ・クライアントを認証する。

【解決手段】　ウェブ・サーバによるウェブ・クライアントからのユーザＩＤ及びパスワードの受信に応答して、ログイン・プロトコルがセキュリティ・サービスで実行される。ユーザが認証され得る場合、資格証明のデータベースに記憶され、ウェブ・サーバがウェブ・クライアントに、固有の識別子を有する持続クライアント状態オブジェクトを戻す。ウェブ・クライアントが続く要求を分散ファイル・システムにすると、識別子を含む持続クライアント状態オブジェクトが、ユーザＩＤ及びパスワードに代用され、セッションをより一層安全にする。この操作では、クッキー識別子が、資格証明記憶テーブルに対するポインタとして使用され、資格証明が次に検索され、分散ファイル・システムからの複数のファイル・アクセスを容易にする。



【特許請求の範囲】
【請求項１】分散コンピュータ環境の分散ファイル・システムに接続可能なウェブ・サーバに、クライアントを認証する方法であって、前記分散コンピュータ環境が、前記分散ファイル・システムへのアクセスを認証されたユーザに、資格証明を戻すセキュリティ・サービスを含むものにおいて、
ａ）前記ウェブ・サーバによる前記クライアントからのユーザＩＤ及びパスワードの受信に応答して、ログイン・プロトコルを前記セキュリティ・サービスで実行し、その結果生じる資格証明を記憶するステップと、
ｂ）前記クライアントに、識別子を有する持続クライアント状態オブジェクトを戻すステップと、
ｃ）前記クライアントが、前記ユーザＩＤ及びパスワードの代わりに、前記識別子を含む前記持続クライアント状態オブジェクトを使用することにより、前記分散ファイル・システム内のウェブ文書への続くアクセスを獲得するステップと、を含む、方法。
【請求項２】前記持続クライアント状態オブジェクト内の前記識別子が、前記記憶するステップで記憶された資格証明を検索するために使用される、請求項１記載の方法。
【請求項３】前記ユーザＩＤ及びパスワードがＨＴＭＬ書式により前記ウェブ・サーバに提供される、請求項１記載の方法。
【請求項４】前記ＨＴＭＬ書式が前記クライアントのユーザにより完成される、請求項３記載の方法。
【請求項５】分散コンピュータ環境の分散ファイル・システムに接続可能なウェブ・サーバに、ウェブ・クライアントを認証する方法であって、前記分散コンピュータ環境が、前記分散ファイル・システムへのアクセスを認証されたユーザに、資格証明を戻すセキュリティ・サービスを含むものにおいて、
ａ）前記ウェブ・サーバにより受信されるＨＴＴＰ要求に応答して、前記ウェブ・クライアントが、持続クライアント状態オブジェクトをサポートするブラウザを有するか否かを判断するステップと、
ｂ）前記ウェブ・クライアントが、前記持続クライアント状態オブジェクトをサポートするブラウザを有する場合、前記ウェブ・サーバが前記ウェブ・クライアントにログインＨＴＭＬ書式、及び前記ＨＴＴＰ要求により識別されるＵＲＬを含む第１の持続クライアント状態オブジェクトを送信するステップと、
ｃ）前記ユーザが前記ＨＴＭＬ書式をユーザＩＤ及びパスワードにより完成するステップと、
ｄ）完成した書式を、前記ＵＲＬを含む前記第１の持続クライアント状態オブジェクトと一緒に、前記ウェブ・サーバに返送するステップと、
ｅ）前記完成した書式から情報を抽出し、ログイン・プロトコルを前記セキュリティ・サービスで実行して、資格証明を生成するステップと、
ｆ）前記ウェブ・クライアントに、識別子を有する第２の持続クライアント状態オブジェクトを戻すステップと、
ｇ）前記ウェブ・クライアントが、ユーザＩＤ及びパスワードの代わりに、前記識別子を含む前記第２の持続クライアント状態オブジェクトを使用することにより、前記分散ファイル・システム内のウェブ文書への続くアクセスを獲得するステップと、を含む、方法。
【請求項６】前記識別子が前記資格証明をアクセスするために使用される、請求項５記載の方法。
【請求項７】分散コンピュータ環境の分散ファイル・システムに接続可能なウェブ・サーバに、ウェブ・クライアントを認証する方法であって、前記分散コンピュータ環境が、前記分散ファイル・システムへのアクセスを認証されたユーザに、資格証明を戻すセキュリティ・サービスを含むものにおいて、
ａ）前記ウェブ・クライアントからのトランザクション要求の受信に応答して、ログイン・プロトコルを前記セキュリティ・サービスで実行し、前記ウェブ・クライアントが前記分散ファイル・システムへのアクセス権を有するか否かを判断するステップと、
ｂ）前記ウェブ・クライアントが前記分散ファイル・システムへのアクセス権を有さない場合、エラー・メッセージを前記ウェブ・クライアントに戻すステップと、
ｃ）前記ウェブ・クライアントが前記分散ファイル・システムへのアクセス権を有する場合、前記ログイン・プロトコルの結果生成される資格証明を、認証済みユーザに関連付けられる資格証明のデータベースに記憶するステップと、
ｄ）前記ウェブ・クライアントに、前記ウェブ・クライアントに固有に関連付けられる識別子を有するクッキーを戻すステップと、
ｅ）前記クライアントが、ユーザＩＤ及びパスワードの代わりに前記クッキーを使用することにより、前記分散ファイル・システム内のウェブ文書への続くアクセスを獲得するステップと、
を含む、方法。
【請求項８】前記クッキー内の前記識別子が、前記データベースから前記記憶するステップで記憶された資格証明を検索するために使用される、請求項７記載の方法。
【請求項９】分散コンピュータ環境の分散ファイル・システムに接続可能なウェブ・サーバに、ウェブ・クライアントを認証する方法であって、前記分散コンピュータ環境が、前記分散ファイル・システムへのアクセスを認証されたユーザに、資格証明を戻すセキュリティ・サービスを含むものにおいて、
前記分散ファイル・システムへのアクセスを認証されたユーザの前記資格証明を、記憶装置に保持するステップと、

前記ウェブ・クライアントからの、識別子を有する持続クライアント状態オブジェクトの受信に応答して、前記識別子を用いて、前記記憶装置内の資格証明の１つをアクセスするステップと、
前記資格証明を用いて、前記分散ファイル・システム内のファイルをアクセスするステップと、
を含む、方法。
【請求項１０】分散コンピュータ環境の分散ファイル・システムに接続可能なウェブ・サーバに、ウェブ・クライアントを認証するために使用されるコンピュータ・プログラム製品であって、前記分散コンピュータ環境が、前記分散ファイル・システムへのアクセスを認証されたユーザに、資格証明を戻すセキュリティ・サービスを含むものにおいて、
コンピュータ読出し可能記憶媒体と、
前記コンピュータ読出し可能記憶媒体に記憶されたプログラム・データとを含み、前記プログラム・データが、
前記ウェブ・サーバによる前記ウェブ・クライアントからのユーザＩＤ及びパスワードの受信に応答して、ログイン・プロトコルを前記セキュリティ・サービスで実行し、その結果生じる資格証明を記憶する手段と、
前記ウェブ・クライアントに、識別子を有する持続クライアント状態オブジェクトを戻す手段と、
前記識別子を含む前記持続クライアント状態オブジェクトの受信に応答して、前記分散ファイル・システム内のウェブ文書への続くアクセスを制御する手段と、
を含む、コンピュータ・プログラム製品。
【請求項１１】前記プログラム・データが、前記ログイン・プロトコルに応答してエラー・メッセージを生成する手段を含む、請求項１０記載のコンピュータ・プログラム製品。
【請求項１２】前記プログラム・データが、前記分散ファイル・システムに認証されたユーザの前記資格証明の記憶を確立する手段を含む、請求項１０記載のコンピュータ・プログラム製品。
【請求項１３】前記持続クライアント状態オブジェクトがクッキーである、請求項１０記載のコンピュータ・プログラム製品。
【請求項１４】分散コンピュータ環境の分散ファイル・システムに接続可能なウェブ・サーバに、ウェブ・クライアントを認証するために使用されるコンピュータ・プログラム製品であって、前記分散コンピュータ環境が、前記分散ファイル・システムへのアクセスを認証されたユーザに、資格証明を戻すセキュリティ・サービスを含むものにおいて、
コンピュータ読出し可能記憶媒体と、
前記コンピュータ読出し可能記憶媒体に記憶されたプログラム・データとを含み、前記プログラム・データが、
前記分散ファイル・システムへのアクセスを認証されたユーザの前記資格証明の記憶を保持する手段と、
前記ウェブ・クライアントからの、識別子を有する持続クライアント状態オブジェクトの受信に応答して、前記識別子を用いて、前記記憶内の前記資格証明の１つをアクセスすることにより、前記分散ファイル・システム内のウェブ文書のアクセスを可能にする手段と、
を含む、コンピュータ・プログラム製品。
【請求項１５】分散ファイル・システムへのアクセスを認証されたユーザに、資格証明を戻すためのセキュリティ・サービスを含む、分散コンピュータ環境に接続可能なコンピュータであって、
プロセッサと、
オペレーティング・システムと、
無国籍コンピュータ・ネットワークを介して、ウェブ・サーバ・プログラムに接続可能なウェブ・クライアントに、ワールド・ワイド・ウェブ情報検索を提供するウェブ・サーバ・プログラムと、
前記ウェブ・クライアントを前記ウェブ・サーバ・プログラムに認証するサーバ・プラグインとを含み、前記サーバ・プラグインが、
前記ウェブ・サーバによる前記ウェブ・クライアントからのユーザＩＤ及びパスワードの受信に応答して、ログイン・プロトコルを前記セキュリティ・サービスで実行し、その結果生じる資格証明を記憶する手段と、
前記ウェブ・クライアントに、識別子を有する持続クライアント状態オブジェクトを戻す手段と、
ユーザＩＤ及びパスワードの代わりに、前記識別子を含む前記持続クライアント状態オブジェクトの続く受信に応答して、前記分散ファイル・システム内のウェブ文書へのアクセスを制御する手段と、
を含む、コンピュータ。
【請求項１６】前記制御する手段が前記識別子を用いて、前記資格証明をアクセスする、請求項１５記載のコンピュータ。
【請求項１７】ウェブ・サーバ、及び前記ウェブ・サーバが接続される分散ファイル・システムから文書をアクセスする方法であって、分散コンピュータ環境内でサポートされる前記分散ファイル・システムが、前記分散ファイル・システムへのアクセスを認証されたユーザに、資格証明を戻すセキュリティ・サービスを有するものにおいて、
ａ）前記ウェブ・サーバによる前記ウェブ・クライアントからのユーザＩＤ及びパスワードの受信に応答して、ログイン・プロトコルを前記セキュリティ・サービスで実行し、その結果生じる資格証明を記憶するステップと、
ｂ）前記ウェブ・クライアントに、識別子を有する持続クライアント状態オブジェクトを戻すステップと、
ｃ）前記クライアントが、前記ユーザＩＤ及びパスワードの代わりに、前記識別子を含む前記持続クライアント状態オブジェクトを使用することにより、前記分散ファ

イル・システム内のウェブ文書へのアクセスを獲得するステップと、
ｄ）前記ウェブ・クライアントが、前記ユーザＩＤ及びパスワードを用いて、前記ウェブ・サーバ内のウェブ文書へのアクセスを獲得するステップと、を含む、方法。
【請求項１８】前記分散ファイル・システムの使用を認証されたユーザの前記資格証明の記憶を保持するステップを含む、請求項１７記載の方法。
【請求項１９】前記識別子が前記記憶から前記資格証明を検索するために使用される、請求項１８記載の方法。
【請求項２０】前記ログイン・プロトコルが不成功の場合、前記ウェブ・サーバから前記ウェブ・クライアントに特注のエラー・メッセージを提供するステップを含む、請求項１７記載の方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は一般に、ウェブ・トランザクション処理に関し、特に安全な分散ファイル・システムに記憶されるウェブ文書へのアクセスを可能にすることに関する。
【０００２】
【従来の技術】インターネットのワールド・ワイド・ウェブは、コンピュータの歴史において、最も成功した分散アプリケーションである。ウェブ環境では、クライアント・マシンが、ウェブ・サーバへのトランザクションのためにハイパテキスト転送プロトコル（ＨＴＴＰ）を使用し、これはハイパテキスト・マークアップ言語（ＨＴＭＬ）として知られる標準のページ記述言語を用いて、ファイル（例えばテキスト、グラフィックス、イメージ、音、ビデオなど）へのユーザ・アクセスを提供する既知のアプリケーション・プロトコルである。ＨＴＭＬは基本文書のフォーマット化を提供し、開発者が他のサーバ及びファイルへの"リンク"を指定することを可能にする。インターネットの範例では、サーバへのネットワーク経路が、ネットワーク接続を定義する特殊な構文を有する、いわゆるユニフォーム・リソース・ロケータ（ＵＲＬ）により識別される。クライアント・マシンにおけるＨＴＭＬ互換のブラウザ（例えばネットスケープ・ナビゲータ）の使用は、ＵＲＬを介するリンクの指定を含む。それに応じてクライアントはリンク内で識別されるサーバに要求を出し、見返りにＨＴＭＬに従いフォーマットされた文書を受信する。
【０００３】多くの組織が、分散コンピュータ環境内で相互接続される複数のコンピュータを使用し、そこではユーザが分散資源をアクセスし、アプリケーションを処理する。ＤＣＥと呼ばれる既知の分散コンピュータ環境は、ＯＳＦ（Open Systems Foundation）から入手可能なソフトウェアを用いて実現されてきた。ＤＣＥ環境が企業における解決法として選択されるようになると、データ共用、印刷サービス、及びデータベース・アクセスなどの分散サービスを提供するために、多くのアプリケーションが利用され得る。ＯＳＦ　ＤＣＥは、これらの環境において使用される分散ファイル・サービス（ＤＦＳ）と呼ばれる分散ファイル・システムを含む。
【０００４】ＤＦＳは独立型のファイル・サーバに勝る多くの利点を提供する。それらには、データ及び資源の高い可用性、超大規模システム全体に渡って情報を共用する能力、及び確固たるＤＣＥセキュリティ機構による情報の保護などが含まれる。特に、ＤＦＳは複製を通じてファイルを高度に使用可能にし、ファイルが配置されるマシンの１つが故障しても、ファイルのコピーをアクセスすることを可能にする。ＤＦＳはまた、様々なファイル・システムに記憶される全てのファイルを、大域ネーム空間に寄せ集める。複数のサーバがそれらのファイル・システムを、このネーム空間にエクスポートすることができる。全てのＤＦＳユーザが間もなくこのネーム空間を共用し、全てのＤＦＳファイルが任意のＤＦＳクライアント・マシンから容易に使用可能になる。
【０００５】ＤＦＳ（または他の類似の分散ファイル・システム）のスケーラビリティ、ファイル可用性、及びセキュリティ機構を利用するために、企業環境において既存の独立型のウェブ・サーバの機能を拡張することが非常に望ましい。副産物として、オフザシェルフの（すなわち既製の）ブラウザを有するユーザは、クライアント・マシン上の追加のソフトウェア無しに、ＤＦＳネーム空間に記憶されるウェブ情報を容易にアクセスすることができる。しかしながら、この目標が達成されるためには、ウェブ・サーバにより提供されるセキュリティ機構を従来のＤＦＳセキュリティと統合することが必要である。別の方法の１つは、（ウェブ・サーバにより提供される）基本認証（Basic Authentication）機構を使用し、各ＨＴＴＰ要求に対してユーザＩＤ及びパスワードを獲得することである。しかしながら、ＤＦＳの状況において、既知の基本認証機構を使用することには、幾つかの問題がある。
【０００６】
【発明が解決しようとする課題】特に、ユーザＩＤ及びパスワードは、あらゆる要求に対して渡される。従って、それらは、たとえパスワードが特定の暗号化機構（例えばＳＳＬ）により保護されるとしても、侵入者により攻撃されがちである。第２に、ＤＦＳ及びウェブ・サーバ・セキュリティ機構が共存することは困難である。ブラウザは特定のサーバに送信されるユーザＩＤ及びパスワードを記憶し、ユーザＩＤ及びパスワードが、そのサーバに送信されるあらゆるＨＴＴＰ要求に付加される。ウェブ・サーバに分散ファイル・システムをアクセスさせる機構が提供される場合、ウェブ・サーバは、サーバ・ローカル・ディレクトリ上に記憶される文書（ウェブ・サーバ・セキュリティにより保護される）、及びＤＦＳ上に記憶される文書（ＤＦＳセキュリティに

より保護される）の両方を保持することになる。ブラウザから見ると、ウェブ・サーバは単一サーバであり、そのウェブ・サーバに対する１対のユーザＩＤ及びパスワードを記憶するだけである。ユーザがＤＦＳ文書及びウェブ・サーバ文書の両方をブラウズしている場合、ユーザはＤＦＳ文書からウェブ・サーバ文書への切り替え、及びその逆の度に、ユーザＩＤ及びパスワードを催促されることになる。最後に、ＤＦＳ認証が失敗する場合、制限されたエラー情報だけがユーザに戻され得る。

【０００７】これらの問題は、ウェブ・サーバ及びＤＦＳセキュリティ機構を統合する上で、既知の基本認証機構を不適当なものにする。本発明はこの問題を解決するものである。

【０００８】本発明の第１の目的は、インターネット・ワールド・ワイド・ウェブ・サーバを通じて、分散ファイル・システムをアクセスするユーザを認証することである。

【０００９】本発明の別の目的は、ユーザがウェブ・サーバを通じて初めてファイル・システムにログインするときに、ユーザＩＤ及びパスワードの転送だけを要求する、ウェブ・ブラウジングのための分散ファイル・システム認証機構を提供することである。続く要求に対しては、"クッキー（cookie）"に記憶される機密ハンドルが、ウェブ・ブラウザからウェブ・サーバに転送される。

【００１０】更に本発明の別の目的は、持続クライアント状態ＨＴＴＰクッキー認証機構を使用することにより、分散ファイル・システムからの安全なウェブ文書アクセスを容易にすることである。

【００１１】更に本発明の別の目的は、ユーザがＤＦＳ文書からウェブ・サーバ文書に切り替えるときに、ユーザが既にＤＦＳにログイン済みであれば、ユーザＩＤ及びパスワードを催促されないように、既知の基本認証セキュリティ機構と共存する、ＤＦＳウェブ・サーバ・アプリケーションのためのクッキー・ベースの認証機構を実現することである。

【００１２】更に本発明の別の目的は、既知の基本認証機構により提供されるエラー・メッセージの代わりに、ウェブ・サーバからブラウザに転送されるカストマイズされたエラー・メッセージを提供することである。

【００１３】本発明のより一般的な目的は、ウェブ・サーバにより提供されるセキュリティ機構を、従来のＤＦＳセキュリティと統合することである。このことは、企業環境において既存の独立型のウェブ・サーバの機能を、ＤＦＳ（または他の類似の分散ファイル・システム）のスケーラビリティ、ファイル可用性、及びセキュリティ機構を利用するように向上させる。副産物として、オフザシェルフのブラウザを有するユーザは、クライアント・マシン上の追加のソフトウェア無しに、ＤＦＳネーム空間に記憶されるウェブ情報を容易にアクセスすることができる。

【００１４】

【課題を解決するための手段】本発明のこれらの及び他の目的が、分散コンピュータ環境の分散ファイル・システムに接続可能なウェブ・サーバに、ウェブ・クライアントを認証する方法により提供される。分散コンピュータ環境が分散ファイル・システムへのアクセスを認証されたユーザに、資格証明を戻すセキュリティ・サービスを含む。ウェブ・サーバによるウェブ・クライアントからのユーザＩＤ及びパスワードの受信に応答して、ログイン・プロトコルがセキュリティ・サービスで実行される。ユーザが認証され得る場合、資格証明が認証済みユーザに関連付けられる資格証明のイン・メモリ資格証明データベースに記憶される。次にウェブ・サーバがウェブ・クライアントに、固有の識別子を有する持続クライアント状態オブジェクトを戻す。このオブジェクトは時にクッキーとして参照されるが、これが次に、ウェブ・クライアントが分散ファイル・システム内のウェブ文書をブラウズすることを可能にするために使用される。特に、ウェブ・クライアントが続く要求を分散ファイル・システムに発行することを希望する場合、識別子を含む持続クライアント状態オブジェクトが、ユーザＩＤ及びパスワードの代わりに使用され、このことがセッションをより一層安全なものにする。この操作では、クッキー識別子がイン・メモリ資格証明データベースに対するポインタとして使用され、資格証明が次に検索され、分散ファイル・システムからの複数のファイル・アクセスを容易にするために使用される。

【００１５】同時にウェブ・クライアントは依然、ＨＴＴＰ要求内の従来のユーザＩＤ及びパスワードを介して（分散ファイル・システム文書とは対照的に）ウェブ・サーバ文書へのアクセスを獲得し得る。

【００１６】本発明の好適な方法によれば、初期ＨＴＴＰ要求に応答して、ウェブ・クライアントが持続クライアント状態オブジェクトすなわち"クッキー"をサポートするブラウザを有するか否かが最初に判断される。有する場合、ウェブ・サーバがウェブ・クライアントにログインＨＴＭＬ書式、及びＨＴＴＰ要求により識別されるＵＲＬを含む第１のクッキーを送信する。ユーザは次に、彼のユーザＩＤ及びパスワードにより、ＨＴＭＬ書式を完成するように催促される。その後、ウェブ・クライアントは、完成した書式を第１のクッキーと一緒にウェブ・サーバに返送する。ウェブ・サーバにおいて、完成した書式から情報が抽出され、分散ファイル・システムのログイン・プロトコルに供給される。ログインが成功すると、ユーザ資格証明が生成され、好適にはイン・メモリ資格証明データベースに記憶される。ログインが不成功の場合、エラー・メッセージがウェブ・クライアントに戻される。次に、認証済みユーザに対し固有識別子が生成され、これが資格証明データベースに対するポ

インタとして使用される。この識別子が次に、ウェブ・クライアントに送信される新たなクッキー内に配置される。新たなクッキーが次にウェブ・クライアントにより、分散ファイル・システムへのあらゆる続くファイル・アクセスのために使用される。新たなクッキーを使用することにより、ウェブ・クライアントは繰り返しユーザＩＤ及びパスワードをネットワークを通じて転送する必要がない。しかしながら、クライアントは依然ユーザＩＤ及びパスワードを使用し、（分散ファイル・システムとは対照的に）ウェブ・サーバからの単純なファイル・アクセスを獲得することができる。

【００１７】前述の説明は、本発明の関連する目的及び特徴の幾つかの概略を述べたものである。これらの目的は、単に本発明の優れた特徴及びアプリケーションの幾つかを表すものであり、後述のように、多くの他の有用な結果が、開示される本発明を別様に適用することにより、または本発明を変更することにより、獲得され得る。従って、本発明の他の目的及び完全な理解が、後述の本発明の実施の形態を参照することにより、得られることであろう。

【００１８】

【発明の実施の形態】本発明が実現される代表的なシステムが、図１に示される。クライアント・マシン１０は、通信チャネル１４を介してウェブ・サーバ・プラットフォーム１２に接続される。説明の都合上、通信チャネル１４はインターネット若しくはイントラネット、または他の既知の接続である。インターネットの場合、ウェブ・サーバ・プラットフォーム１２は、クライアントによりアクセス可能な複数のサーバの１つであり、クライアントの１つがマシン１０により示される。クライアント・マシンはブラウザ１６を含み、これはネットワークのサーバをアクセスするために使用される既知のソフトウェア・ツールである。一例として、クライアント・マシンはパーソナル・コンピュータである。代表的なブラウザには、ネットスケープ・ナビゲータ（全バージョン）、マイクロソフト・インターネット・エクスプローラ（全バージョン）などが含まれ、これらの各々は"オフザシェルフの"またはダウンロード可能なソフトウェア・プログラムである。ウェブ・サーバ・プラットフォーム（時に"ウェブ"・サイトとして参照される）は、ファイルをハイパテキスト文書及びオブジェクトの書式でサポートする。インターネットの範例では、サーバへのネットワーク経路が、いわゆるユニフォーム・リソース・ロケータ（ＵＲＬ）により識別される。ワールド・ワイド・ウェブは、インターネットのマルチメディア情報検索システムである。特に、これはハイパテキスト転送プロトコル（ＨＴＴＰ）を使用するインターネットのサーバの集合であり、ＨＴＴＰはハイパテキスト・マークアップ言語（ＨＴＭＬ）を用いて、ファイルへのユーザ・アクセスを提供する。

【００１９】代表的なウェブ・サーバ・プラットフォーム１２は、ＩＢＭ　ＲＩＳＣ　Ｓｙｓｔｅｍ／６０００コンピュータ１８を含み、これはＡＩＸ（拡張対話式エグゼクティブ・バージョン４．１以上）オペレーティング・システム２０、及びインタフェース拡張をサポートするネットスケープ・エンタプライズ・バージョン２．０などの、ウェブ・サーバ・プログラム２２を実行する。ウェブ・サーバ・プラットフォーム１２は更に、管理のためのグラフィカル・ユーザ・インタフェース（ＧＵＩ）２４を含む。ＲＩＳＣベースのコンピュータの様々なモデルが、ＩＢＭの多くの刊行物、例えば"RISC System/6000、013 and 7016 POWERstation and POWERserver Hardware Technical Reference"、注文番号SA23-2644-00で述べられている。ＡＩＸ　ＯＳは、ＩＢＭ発行の"AIX Operating System TechnicalReference"（第１版、１９８５年１１月）などで述べられている。上記のプラットフォームが有用であるが、任意の他の適切なハードウェア／オペレーティング・システム／ウェブ・サーバの組み合わせが使用され得る。

【００２０】ウェブ・サーバはクライアント要求を受諾し、応答を戻す。ウェブ・サーバ１８の操作は、多数のサーバ・アプリケーション機能（ＳＡＦ）により管理され、各ＳＡＦはシーケンスの特定のステップにおいて実行されるように構成される。このシーケンスが図２に示され、許可変換（authorization translation）ステップ３０で開始し、その間にサーバがクライアントにより送信される任意の許可情報を、ユーザ及びグループに変換する。必要に応じて許可変換ステップはメッセージを復号して、実際のクライアント要求を獲得する。ステップ３２はネーム変換と称され、要求に関連付けられるＵＲＬがそのまま維持されるか、またはシステム依存のファイル・ネーム、リダイレクトＵＲＬまたはミラー・サイトＵＲＬに変換され得る。ステップ３４は経路チェックと称され、サーバが結果の経路に様々なテストを実行し、所与のクライアントが文書を検索し得るように保証する。ステップ３６は、時にオブジェクト・タイプとして参照され、所与の文書に対するＭＩＭＥ（多目的インターネット・メール拡張）タイプ情報（例えばテキスト／html、イメージ／gifなど）が識別される。ステップ３８はサービスと称され、ウェブ・サーバ・ルーチンが内部サーバ機能を選択し、結果を正規のサーバ・サービス・ルーチンを介してクライアントに返送する。選択される特定の機能は、要求の性質に依存する。ステップ４０はログ追加と称され、トランザクションに関する情報が記録される。ステップ４２はエラーと称され、エラーに遭遇するとき、サーバがクライアントに応答する。これらの操作の詳細については、ネットスケープ社発行の"Web Server Programmer's Guide"、Chapter 5で述べられている。

【００２１】ウェブ・サーバ１８は、サーバ・アプリケ

ーション機能（ＳＡＦ）の既知のセットを含む。これらの機能はクライアントの要求及びサーバの他の構成データを入力として受け取り、応答をサーバに出力として戻す。図１を再度参照すると、ウェブ・サーバ１８はアプリケーション・プログラミング・インタフェース（ＡＰＩ）２６を含み、これはアプリケーション開発者が、一般に"プラグイン"として参照されるソフトウェア・プログラムを通じて、コア機能（すなわちＳＡＦ）を拡張及び（または）カストマイズすることを可能にする拡張を提供する。本発明はサーバＡＰＩ２６を利用し、ユーザの認証を容易にするプラグインを提供するものであり、それによりクライアント・マシン１０のユーザは、ブラウザを用いて分散ファイル・システム５０上の文書へのウェブ・アクセスが可能になる。

【００２２】特に本発明の一般的な目的によれば、クライアント・マシン１０のユーザが、（意図的にまたは無意識に）オフザシェルフのブラウザ１６を使用し、分散ファイル・システム５０内に配置される文書をアクセス、ブラウズ及び検索することを可能にする。１つのこうしたファイル・システム５０は、分散ファイル・サービス（ＤＦＳ）であり、これは分散コンピュータ環境（ＤＣＥ）と称されるネットワーク環境において実現される、既知の分散ファイル・システムである。ＤＣＥはＯＳＦから入手可能なソフトウェアを用いて実現される。分散コンピュータ環境では、マシンのグループが通常、"ドメイン"として参照される。ＯＳＦ　ＤＣＥドメインは、"セル"と呼ばれる。ＤＣＥセルは、たくさんの位置に存在する数百のマシンを含む複雑な環境であり得る。

【００２３】ＤＣＥ　ＤＦＳ５０は、ネーミングのために遠隔プロシージャ呼び出し（ＲＰＣ）を、また認証サービスのためにＤＣＥセキュリティ・サービス５２を利用することにより、データ共用サービスを提供する。ＤＦＳ５０はセッション・マネージャ・プロセス２７を介して、ＤＣＥセキュリティ・サービス５２とインタフェースする。これに関しては、米国特許出願第０８／７９００４２号で詳述されている。ＤＣＥサービスの利用に加え、ＤＦＳ自身の機構は豊富である。ＤＦＳは一様な大域ファイル空間を提供し、このことは全てのＤＦＳクライアント・ユーザが同一のファイル空間を眺望することを可能にし、またクライアントにおいてファイル・システム・データをキャッシュすることにより、ファイル・サーバへのネットワーク・トラフィックを低減し、スケーラビリティ及び性能を改善する。ＤＦＳはまた、通知ファイル・ロッキング、及びオペレーティング・システムのネイティブ・ファイル・システムをエクスポートする能力における機構の１つをサポートする。例えば、ＡＩＸオペレーティング・システムの場合、ネイティブ・ファイル・システムはジャーナルド・ファイル・システム（ＪＦＳ）である。更にＤＦＳはそれ自身の物理ファイル・システム、すなわちＤＣＥローカル・ファイル・システム（ＬＦＳ）を提供する。ＤＣＥ　ＬＦＳは、データへのアクセスを保護するためのファイル及びディレクトリに関するＤＣＥアクセス制御リスト（ＡＣＬ）のサポート、並びに複製及び負荷平衡化などの高度データ管理能力を提供する。

【００２４】ＤＦＳ５０は、いわゆるＤＣＥケルベロス・ベース（Kerberos-based）の認証を使用する。ＵＮＩＸの"資格証明"が、各ファイル操作に関連付けられ、その操作のローカル認証情報を保持する。特に、資格証明は、特定のマシン（またはマルチユーザ・マシン上のユーザ）を定義するデータ構造である。ローカル・オペレーティング・システムの観点から、資格証明はユーザＩＤ、グループＩＤ、任意的にオペレーティング・システムの特権のリスト、及びＰＡＧ（プロセス認証グループ）として知られる認証識別子を含む。ＰＡＧは、ＤＦＳ５０とＤＣＥセキュリティ・サービス５２との間で、"チケット"を関連付けるタグとして機能する。ＤＦＳユーザが、dce_loginとして既知のＤＣＥログイン機構を介して認証するとき、ＤＣＥセキュリティ・サービスが（ネットワークを介して）ＤＦＳとsetpag()インタフェースを通じて対話し、プロセスの資格証明におけるＰＡＧ／チケット関係を確立する。ファイル・システム要求に際してＤＦＳは資格証明構造からＰＡＧを抽出し、ＤＦＳファイル・サーバへのＲＰＣ要求に対してＤＣＥユーザの認証を確立する。

【００２５】本発明に関連付けられる制御フローが、図３のプロセス・フロー図に示される。この図は図１の基本システムを示し、関連データベース５８を有するアカウント・マネージャ５６を含む。セッション・マネージャ２７は、ウェブ・サーバの初期化時に始動し、好適にはワークステーション・コンピュータ１８により実行される。セッション・マネージャ２７は、それ自身の記憶域２９を含む。クライアント１０が（ブラウザ１６を通じて）ＤＦＳ文書を要求するとき（ステップａ）、ウェブ・サーバ２２が（ＳＡＦプラグイン２５を用いて、）サーバ経路チェックを呼び出す（ステップｂ）。経路チェックは、セッション・マネージャ２７により、ユーザが適切なＤＣＥ資格証明を有するか否かを判断する。否定の場合（ステップｃ）、ＳＡＦプラグイン２５がエラー・メッセージ（例えば"４０１；無許可"）をブラウザ１６に戻し（ステップｄ）、ユーザにユーザＩＤ及びパスワードを催促する。ユーザからユーザＩＤ及びパスワードを獲得した後（ステップｅ）、ＳＡＦプラグイン２５がセッション・マネージャ２７を呼び出し（ステップｆ）、ユーザのＤＣＥ資格証明を獲得する。セッション・マネージャ２７がＤＣＥ資格証明をウェブ・サーバ２２に戻す（ステップｇ）。サーバは次に、ユーザを表すこのユーザ資格証明を使用し、ＤＦＳ５０に記憶される文書を検索する（ステップｈ）。文書を検索後、（好適

には別のＡＰＩプラグインを用いて、）アカウント・マネージャ５６が呼び出され（ステップｉ）、適切な使用情報をデータベース５８に保管する（ステップｊ）。

【００２６】ユーザがＤＦＳファイルをアクセスしようと試行するとき、セッション・マネージャ２７がウェブ・サーバにより呼び出される。ユーザが既にＤＣＥにより認証されている場合、セッション・マネージャ２７がユーザ資格証明をサーバに戻し、サーバはこの資格証明を使用し、ユーザのためにＤＦＳ文書を検索する。ユーザが認証されていない場合には、セッション・マネージャ２７がユーザのためにログインし、ＤＣＥセキュリティから資格証明を獲得する。セッション・マネージャはインメモリ・データベースを保持して、ログインしたユーザを追跡し、それによりユーザは複数のＤＦＳページをアクセスできる。

【００２７】基本認証機構を使用する代わりに、本発明は持続クライアント状態ＨＴＴＰクッキーを使用する。クッキーは、クライアント側の情報を記憶及び検索するために、サーバ側の接続（ＣＧＩスクリプトなど）が使用することのできる既知のインターネット機構である。サーバはまた、ＨＴＴＰオブジェクトをクライアントに戻すとき、状態情報も送信し得る。クライアントはこの状態情報を記憶する。通常、"クッキー"と呼ばれる状態オブジェクトは、その状態が有効であるＵＲＬの範囲の記述を含み得る。netscape.comのパス"/newref/std/cookie_spec_html"で見られる"Persistent Client State HTTP Cookies"、Preliminary Specificationによれば、クッキーは通常、ＣＧＩスクリプトを通じて、Set_CookieヘッダをＨＴＴＰ応答の一部として含むことにより、クライアントに導入される。既知のクッキー構文を以下に示す。

【００２８】Set-Cookie ＨＴＴＰ応答ヘッダの構文：これはＨＴＴＰヘッダに、クライアントにより後の検索のために記憶される新たなデータを追加するための、ＣＧＩスクリプトの形式である。

Set-Cookie：NAME=VALUE；expires=DATE；
path=PATH；domain=DOMAIN_NAME；secure

【００２９】NAME=VALUE

このストリングは、セミコロン、カンマ、及び空白を除く文字シーケンスである。こうしたデータをネームまたは値内に配置する必要がある場合、ＵＲＬstyle％ＸＸ符号化などの特定の符号化方法が推奨される。しかしながら、符号化は定義または要求されない。これはSet_Cookieヘッダ上で要求される唯一の属性である。

【００３０】expires=DATE

expires（期限）属性は、そのクッキーの有効寿命を定義するデータ・ストリングを指定する。満了日に達すると、クッキーはもはや記憶または配布されない。日付ストリングは、次のようである。

Wdy、DD-Mon-YYY HH：MM：SS GMT

【００３１】domain=DOMAIN_NAME

有効なクッキーを求めてクッキー・リストを探索するとき、クッキーのdomain（ドメイン）属性が、ＵＲＬがフェッチされるホストのインターネット・ドメイン・ネームと比較される。末尾が一致すると、クッキーは経路マッチングを通じて、それが送信されるべきか否かを確認する。"末尾マッチング"はドメイン属性が、ホストの完全に適格なドメイン・ネームの末尾に対してマッチングされることを意味する。例えば"acme.com"のドメイン属性は、"shipping.crate.acme.com"や、"anvil.acme.com"などのホスト・ネームとマッチングする。

【００３２】指定されるドメイン内のホストだけが、ドメインに対してクッキーをセットでき、ドメインは、".com"、".edu"、及び"va.us"の形式のドメインを回避するために、少なくとも２つまたは３つのピリオドを有さねばならない。次に示す７つの特殊なトップ・レベル・ドメインの１つに入る任意のドメインは、ピリオドを２つだけ必要とする。あらゆる他のドメインは、少なくとも３つのピリオドを必要とする。７つの特殊なトップ・レベル・ドメインは、"COM"、"EDU"、"NET"、"ORG"、"GOV"、"MIL"及び"INT"である。ドメインのデフォルト値は、クッキー応答を生成したサーバのホスト・ネームである。

【００３３】path=PATH

path（経路）属性は、クッキーが有効であるドメイン内のＵＲＬのサブセットを指定するために使用される。クッキーが既にドメイン・マッチングで一致している場合、ＵＲＬの経路ネーム要素が経路属性と比較され、一致が存在する場合、クッキーが有効と見なされ、ＵＲＬ要求と一緒に送信される。経路"/foo"は、"/foobar"及び"/foo/bar.html"と一致する。経路"/"は最も一般的な経路である。経路が指定されない場合には、クッキーを含むヘッダにより記述される文書と同一の経路と仮定される。

【００３４】secure

クッキーがsecure（安全）とマークされる場合、これはホストとの通信チャネルが安全な場合に限り、伝送される。現在、これは安全なクッキーが、ＨＴＴＰＳ（ＳＳＬを介するＨＴＴＰ）サーバにだけ送信されることを意味する。secureが指定されない場合、クッキーは非保護チャネル上を平文で送信されても安全であると見なされる。

【００３５】Cookie ＨＴＴＰ要求ヘッダの構文：ＨＴＴＰサーバからＵＲＬを要求するとき、ブラウザはＵＲＬを全てのクッキーに対してマッチングし、それらのいずれかが一致すると、全ての一致したクッキーのネーム／値の対を含むラインが、ＨＴＴＰ要求に含まれる。そのラインの形式を次に示す。

Cookie：NAME1=OPAQUE_STRING1；NAME2=OPAQUE_STRING2

【００３６】ＨＴＴＰクッキーを利用する本発明の認証

フローを示すフローチャートが、図4に示される。ルーチンは、サーバにより受信される各ＨＴＴＰ要求に対して、ステップ６０で開始する。ステップ６２で、要求がＨＴＴＰクッキーをサポートするブラウザにより送信されたか否かが判断される。例えば、ネットスケープ・ブラウザ（例えばナビゲータ（全バージョン））及びマイクロソフト・ブラウザ（例えばマイクロソフト・インターネット・エクスプローラ（全バージョン））の両者は、クッキーをサポートするが、他の市販のブラウザ・プログラムはサポートしない。ステップ６２のテストの結果が否定の場合、ステップ６４で基本認証がユーザを認証するために使用される。ステップ６２のテスト結果が肯定の場合（すなわち、ブラウザがクッキーをサポートする）、本方法はステップ６６に継続し、要求ヘッダ内に既存のクッキーが含まれるか否かをテストする。ステップ６６のテスト結果が肯定の場合、ユーザは既に認証されており、基本認証が使用される。ステップ６６の結果が否定の場合、ブラウザはクッキーをサポートするが、クッキーがまだ存在しない。

【００３７】ステップ６８では、サーバがログインＨＴＭＬ書式を返送し、ユーザにユーザＩＤ及びパスワードを催促する。サーバはまた、ユーザにより要求される文書のＵＲＬをエントリとして含むクッキーを返送する。特に、上述のように、ユーザＩＤがＤＣＥセキュリティ・サーバにより（セッション・マネージャを介して）認証された後、ウェブ・サーバはユーザのために文書を検索する必要がある。この場合、ウェブ・サーバは文書を検索するためにオリジナルＵＲＬを必要とする。ウェブ・サーバは無国籍なので、ブラウザはオリジナルＵＲＬを提供されなければならない。これはクッキーを提供することにより達成される。ステップ７０で、ユーザはＨＴＭＬ書式にユーザＩＤ及びパスワードを記入する。書式自身は、ＣＧＩスクリプトを用いて既知のように生成される。ステップ７２で、書式内に提供されたユーザＩＤ及びパスワードが、ブラウザがステップ６８で受信したクッキーと一緒にサーバに返送される。

【００３８】ユーザＩＤ及びパスワードを用いて、ルーチンはステップ７４へ継続し、従来のdce_login機構を介してユーザを認証する。既知のように、dce_loginの実行は、ユーザがＤＦＳへのアクセスを獲得するために使用する"資格証明"を生成する。ステップ７６の結果、認証の不成功が判断される場合、サーバはステップ８０で、特定の失敗を記述するカストマイズされたＨＴＭＬ文書をブラウザに返送する。次にステップ８１で、ステップ６８で生成されたクッキーが破壊される。ステップ７６で認証の成功が判断される場合には、ルーチンはステップ７７へ継続し、ユーザの固有のＩＤ（例えばＤＣＥ　ＵＵＩＤ）を生成する。ステップ７８で、（ＤＣＥセキュリティ・サーバへの）ログインにより生成されたＤＦＳ資格証明が、セッション・マネージャに関連付けられるデータベース（好適にはインメモリ記憶）に記憶され、固有のＩＤにより索引付けされる。

【００３９】ルーチンはステップ８２へ継続し、ブラウザにステップ７７で生成された固有のＩＤを含む新たなクッキーを返送する。次にステップ８３で、ステップ６８で生成されたクッキーが破壊される。固有のＩＤは実際には機密ハンドルであり、これはセッション・マネージャに関連付けられるデータベースに記憶される資格証明のテーブルへのエントリである。ブラウザからのサービスに対する続く要求に対しては、固有のＩＤ（ステップ８２でサーバからブラウザに戻された新たなクッキー内でサポートされる）が、このデータベースに記憶されるユーザのＤＦＳ資格証明を指し示すポインタとして使用される。従って、ステップ８４で、サーバは、固有のＩＤを含む新たなクッキーを有する新たな要求を受信する。ステップ８６で、この固有のＩＤがユーザの資格証明を獲得するために使用される。ステップ８８で、資格証明がＤＦＳ内でサポートされるウェブ文書を検索するために（好適にはブラウザを装うウェブ・サーバにより）使用される。

【００４０】ブラウザからの続く要求は、固有のＩＤを有するクッキーを伝送し、従ってステップ８４、８６及び８８が、全ての続く要求に対して繰り返される。従って、本発明によれば、ユーザＩＤ及びパスワードの転送が１度だけ、すなわちユーザが最初にＤＦＳにログインするときに要求される。その後、固有のＩＤを有するクッキーが続く要求に際して転送される。この機構は、ウェブ・サーバにより提供される基本認証セキュリティ機構と共存し得る。ユーザは、ＤＦＳ文書からウェブ・サーバ文書に切り替えるとき、既にＤＣＥセキュリティ・サービスを通じてログインしていれば、ユーザＩＤ及びパスワードを再度催促されない。基本認証機構において指定されるエラー・コードに制限されること無しに、カストマイズされたエラー・メッセージがブラウザに返送され得る。

【００４１】本発明のクッキー・ベースの認証機構の好適な実施例の１つは、コード・モジュール内の命令セット（プログラム・コード）として、コンピュータのランダム・アクセス・メモリに存在する。コンピュータにより要求されるまで、命令セットは別のコンピュータ・メモリ内、例えばハード・ディスク・ドライブ内、または光ディスク（ＣＤ　ＲＯＭドライブで使用される）若しくはフロッピー・ディスク（フロッピー・ディスク・ドライブで使用される）などの取外し可能メモリ内に記憶されたり、或いはコンピュータ・ネットワークを介してダウンロードされてもよい。更に上述された様々な方法は、ソフトウェアにより選択的に活動化または再構成される汎用コンピュータにおいて好都合に実現されるが、当業者には、こうした方法がハードウェア若しくはファームウェアにより、または要求される方法ステップを実

行するように構成された特殊装置により実現され得ることが理解されよう。

【００４２】本明細書で使用されるように、"ウェブ"・クライアントは、インターネットなどのコンピュータ・ネットワークに、直接的または間接的に接続される、または任意の既知のまたは後に開発される様式で接続可能な、任意のコンピュータまたはその構成要素を意味するように広く解釈されるべきである。用語"ウェブ"・サーバもまた、コンピュータ、コンピュータ・プラットフォーム、またはコンピュータ若しくはプラットフォームの付属物、或いはその任意の構成要素を意味するように、広く解釈されるべきである。

【００４３】更に、本発明は特定の分散ファイル・システム環境における好適な実施例に関して述べられてきたが、当業者には、本発明がその趣旨及び範囲内において、変更を伴うことにより、他の異なるハードウェア及びオペレーティング・システム・アーキテクチャにおいても実現され得ることが理解されよう。従って、例えば、本発明は好適にはオフザシェルフのブラウザが、ＤＦＳに記憶されるウェブ文書をアクセス可能なように実現されたが、本発明の原理は、サン・マイクロシステムズ社により開発されたネットワーク・ファイル・システム（ＮＦＳ）はもちろんのこと、（ＤＦＳが導出された）ＡＦＳなどの、他の既知のアーキテクチャにも同様に適用可能である。更にＯＳＦ　ＤＣＥも本発明の必要条件ではない。

【００４４】まとめとして、本発明の構成に関して以下の事項を開示する。

【００４５】（１）分散コンピュータ環境の分散ファイル・システムに接続可能なウェブ・サーバに、クライアントを認証する方法であって、前記分散コンピュータ環境が、前記分散ファイル・システムへのアクセスを認証されたユーザに、資格証明を戻すセキュリティ・サービスを含むものにおいて、

ａ）前記ウェブ・サーバによる前記クライアントからのユーザＩＤ及びパスワードの受信に応答して、ログイン・プロトコルを前記セキュリティ・サービスで実行し、その結果生じる資格証明を記憶するステップと、

ｂ）前記クライアントに、識別子を有する持続クライアント状態オブジェクトを戻すステップと、

ｃ）前記クライアントが、前記ユーザＩＤ及びパスワードの代わりに、前記識別子を含む前記持続クライアント状態オブジェクトを使用することにより、前記分散ファイル・システム内のウェブ文書への続くアクセスを獲得するステップと、を含む、方法。

（２）前記持続クライアント状態オブジェクト内の前記識別子が、前記記憶するステップで記憶された資格証明を検索するために使用される、前記（１）記載の方法。

（３）前記ユーザＩＤ及びパスワードがＨＴＭＬ書式により前記ウェブ・サーバに提供される、前記（１）記載の方法。

（４）前記ＨＴＭＬ書式が前記クライアントのユーザにより完成される、前記（３）記載の方法。

（５）分散コンピュータ環境の分散ファイル・システムに接続可能なウェブ・サーバに、ウェブ・クライアントを認証する方法であって、前記分散コンピュータ環境が、前記分散ファイル・システムへのアクセスを認証されたユーザに、資格証明を戻すセキュリティ・サービスを含むものにおいて、

ａ）前記ウェブ・サーバにより受信されるＨＴＴＰ要求に応答して、前記ウェブ・クライアントが、持続クライアント状態オブジェクトをサポートするブラウザを有するか否かを判断するステップと、

ｂ）前記ウェブ・クライアントが、前記持続クライアント状態オブジェクトをサポートするブラウザを有する場合、前記ウェブ・サーバが前記ウェブ・クライアントにログインＨＴＭＬ書式、及び前記ＨＴＴＰ要求により識別されるＵＲＬを含む第１の持続クライアント状態オブジェクトを送信するステップと、

ｃ）前記ユーザが前記ＨＴＭＬ書式をユーザＩＤ及びパスワードにより完成するステップと、

ｄ）完成した書式を、前記ＵＲＬを含む前記第１の持続クライアント状態オブジェクトと一緒に、前記ウェブ・サーバに返送するステップと、

ｅ）前記完成した書式から情報を抽出し、ログイン・プロトコルを前記セキュリティ・サービスで実行して、資格証明を生成するステップと、

ｆ）前記ウェブ・クライアントに、識別子を有する第２の持続クライアント状態オブジェクトを戻すステップと、

ｇ）前記ウェブ・クライアントが、ユーザＩＤ及びパスワードの代わりに、前記識別子を含む前記第２の持続クライアント状態オブジェクトを使用することにより、前記分散ファイル・システム内のウェブ文書への続くアクセスを獲得するステップと、を含む、方法。

（６）前記識別子が前記資格証明をアクセスするために使用される、前記（５）記載の方法。

（７）分散コンピュータ環境の分散ファイル・システムに接続可能なウェブ・サーバに、ウェブ・クライアントを認証する方法であって、前記分散コンピュータ環境が、前記分散ファイル・システムへのアクセスを認証されたユーザに、資格証明を戻すセキュリティ・サービスを含むものにおいて、

ａ）前記ウェブ・クライアントからのトランザクション要求の受信に応答して、ログイン・プロトコルを前記セキュリティ・サービスで実行し、前記ウェブ・クライアントが前記分散ファイル・システムへのアクセス権を有するか否かを判断するステップと、

ｂ）前記ウェブ・クライアントが前記分散ファイル・システムへのアクセス権を有さない場合、エラー・メッセ

ージを前記ウェブ・クライアントに戻すステップと、
ｃ）前記ウェブ・クライアントが前記分散ファイル・システムへのアクセス権を有する場合、前記ログイン・プロトコルの結果生成される資格証明を、認証済みユーザに関連付けられる資格証明のデータベースに記憶するステップと、
ｄ）前記ウェブ・クライアントに、前記ウェブ・クライアントに固有に関連付けられる識別子を有するクッキーを戻すステップと、
ｅ）前記クライアントが、ユーザＩＤ及びパスワードの代わりに前記クッキーを使用することにより、前記分散ファイル・システム内のウェブ文書への続くアクセスを獲得するステップと、を含む、方法。
（８）前記クッキー内の前記識別子が、前記データベースから前記記憶するステップで記憶された資格証明を検索するために使用される、前記（７）記載の方法。
（９）分散コンピュータ環境の分散ファイル・システムに接続可能なウェブ・サーバに、ウェブ・クライアントを認証する方法であって、前記分散コンピュータ環境が、前記分散ファイル・システムへのアクセスを認証されたユーザに、資格証明を戻すセキュリティ・サービスを含むものにおいて、前記分散ファイル・システムへのアクセスを認証されたユーザの前記資格証明を、記憶装置に保持するステップと、前記ウェブ・クライアントからの、識別子を有する持続クライアント状態オブジェクトの受信に応答して、前記識別子を用いて、前記記憶装置内の資格証明の１つをアクセスするステップと、前記資格証明を用いて、前記分散ファイル・システム内のファイルをアクセスするステップと、を含む、方法。
（１０）分散コンピュータ環境の分散ファイル・システムに接続可能なウェブ・サーバに、ウェブ・クライアントを認証するために使用されるコンピュータ・プログラム製品であって、前記分散コンピュータ環境が、前記分散ファイル・システムへのアクセスを認証されたユーザに、資格証明を戻すセキュリティ・サービスを含むものにおいて、コンピュータ読出し可能記憶媒体と、前記コンピュータ読出し可能記憶媒体に記憶されたプログラム・データとを含み、前記プログラム・データが、前記ウェブ・サーバによる前記ウェブ・クライアントからのユーザＩＤ及びパスワードの受信に応答して、ログイン・プロトコルを前記セキュリティ・サービスで実行し、その結果生じる資格証明を記憶する手段と、前記ウェブ・クライアントに、識別子を有する持続クライアント状態オブジェクトを戻す手段と、前記識別子を含む前記持続クライアント状態オブジェクトの受信に応答して、前記分散ファイル・システム内のウェブ文書への続くアクセスを制御する手段と、を含む、コンピュータ・プログラム製品。
（１１）前記プログラム・データが、前記ログイン・プロトコルに応答してエラー・メッセージを生成する手段を含む、前記（１０）記載のコンピュータ・プログラム製品。
（１２）前記プログラム・データが、前記分散ファイル・システムに認証されたユーザの前記資格証明の記憶を確立する手段を含む、前記（１０）記載のコンピュータ・プログラム製品。
（１３）前記持続クライアント状態オブジェクトがクッキーである、前記（１０）記載のコンピュータ・プログラム製品。
（１４）分散コンピュータ環境の分散ファイル・システムに接続可能なウェブ・サーバに、ウェブ・クライアントを認証するために使用されるコンピュータ・プログラム製品であって、前記分散コンピュータ環境が、前記分散ファイル・システムへのアクセスを認証されたユーザに、資格証明を戻すセキュリティ・サービスを含むものにおいて、コンピュータ読出し可能記憶媒体と、前記コンピュータ読出し可能記憶媒体に記憶されたプログラム・データとを含み、前記プログラム・データが、前記分散ファイル・システムへのアクセスを認証されたユーザの前記資格証明の記憶を保持する手段と、前記ウェブ・クライアントからの、識別子を有する持続クライアント状態オブジェクトの受信に応答して、前記識別子を用いて、前記記憶内の前記資格証明の１つをアクセスすることにより、前記分散ファイル・システム内のウェブ文書のアクセスを可能にする手段と、を含む、コンピュータ・プログラム製品。
（１５）分散ファイル・システムへのアクセスを認証されたユーザに、資格証明を戻すためのセキュリティ・サービスを含む、分散コンピュータ環境に接続可能なコンピュータであって、プロセッサと、オペレーティング・システムと、無国籍コンピュータ・ネットワークを介して、ウェブ・サーバ・プログラムに接続可能なウェブ・クライアントに、ワールド・ワイド・ウェブ情報検索を提供するウェブ・サーバ・プログラムと、前記ウェブ・クライアントを前記ウェブ・サーバ・プログラムに認証するサーバ・プラグインとを含み、前記サーバ・プラグインが、前記ウェブ・サーバによる前記ウェブ・クライアントからのユーザＩＤ及びパスワードの受信に応答して、ログイン・プロトコルを前記セキュリティ・サービスで実行し、その結果生じる資格証明を記憶する手段と、前記ウェブ・クライアントに、識別子を有する持続クライアント状態オブジェクトを戻す手段と、ユーザＩＤ及びパスワードの代わりに、前記識別子を含む前記持続クライアント状態オブジェクトの続く受信に応答して、前記分散ファイル・システム内のウェブ文書へのアクセスを制御する手段と、を含む、コンピュータ。
（１６）前記制御する手段が前記識別子を用いて、前記資格証明をアクセスする、前記（１５）記載のコンピュータ。
（１７）ウェブ・サーバ、及び前記ウェブ・サーバが接

続される分散ファイル・システムから文書をアクセスする方法であって、分散コンピュータ環境内でサポートされる前記分散ファイル・システムが、前記分散ファイル・システムへのアクセスを認証されたユーザに、資格証明を戻すセキュリティ・サービスを有するものにおいて、

ａ）前記ウェブ・サーバによる前記ウェブ・クライアントからのユーザＩＤ及びパスワードの受信に応答して、ログイン・プロトコルを前記セキュリティ・サービスで実行し、その結果生じる資格証明を記憶するステップと、

ｂ）前記ウェブ・クライアントに、識別子を有する持続クライアント状態オブジェクトを戻すステップと、

ｃ）前記クライアントが、前記ユーザＩＤ及びパスワードの代わりに、前記識別子を含む前記持続クライアント状態オブジェクトを使用することにより、前記分散ファイル・システム内のウェブ文書へのアクセスを獲得するステップと、

ｄ）前記ウェブ・クライアントが、前記ユーザＩＤ及びパスワードを用いて、前記ウェブ・サーバ内のウェブ文書へのアクセスを獲得するステップと、を含む、方法。

（１８）前記分散ファイル・システムの使用を認証されたユーザの前記資格証明の記憶を保持するステップを含む、前記（１７）記載の方法。

（１９）前記識別子が前記記憶から前記資格証明を検索するために使用される、前記（１８）記載の方法。

（２０）前記ログイン・プロトコルが不成功の場合、前記ウェブ・サーバから前記ウェブ・クライアントに特注のエラー・メッセージを提供するステップを含む、前記（１７）記載の方法。

【図面の簡単な説明】

【図１】本発明のプラグインが実現される代表的なシステムを示す図である。

【図２】クライアント・マシンのブラウザからの要求の受信に応答する、従来のウェブ・トランザクションのサーバ側の操作のフローチャートを示す図である。

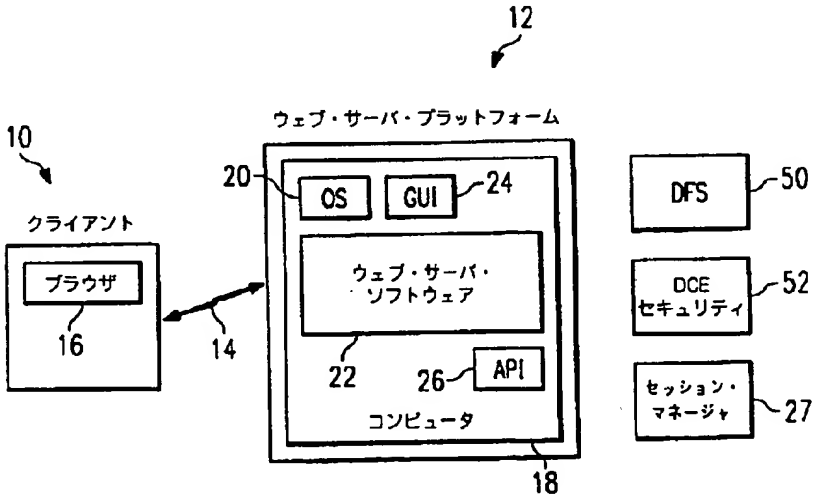
【図３】本発明の教示に従い実現されるウェブ・トランザクションを示すプロセス・フロー図である。

【図４】本発明のプロセス・フローの詳細フローチャートを示す図である。

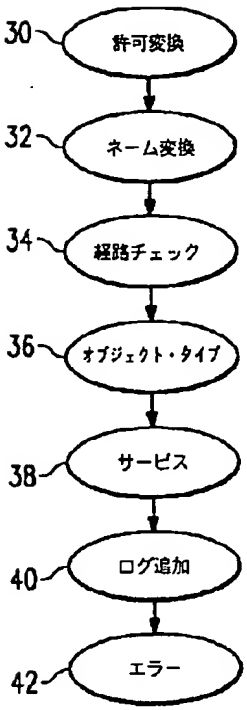
【符号の説明】

１０　クライアント・マシン
１２　ウェブ・サーバ・プラットフォーム
１４　通信チャネル
１６　ブラウザ
１８　コンピュータ
２０　ＡＩＸオペレーティング・システム
２２　ウェブ・サーバ・プログラム
２４　グラフィカル・ユーザ・インタフェース（ＧＵＩ）
２５　ＳＡＦプラグイン
２６　アプリケーション・プログラミング・インタフェース（ＡＰＩ）
２７　セッション・マネージャ
２９　記憶域
５０　分散ファイル・システム
５２　ＤＣＥセキュリティ・サービス
５６　アカウント・マネージャ
５８　データベース

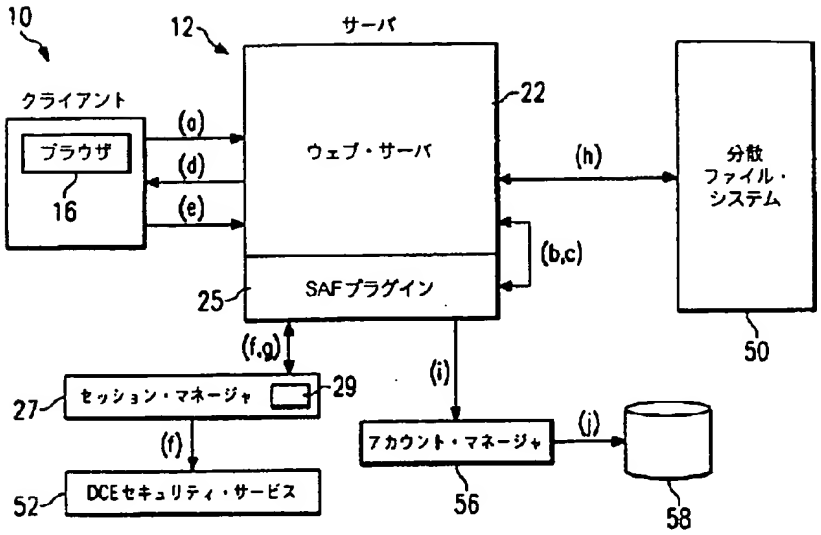
【図１】



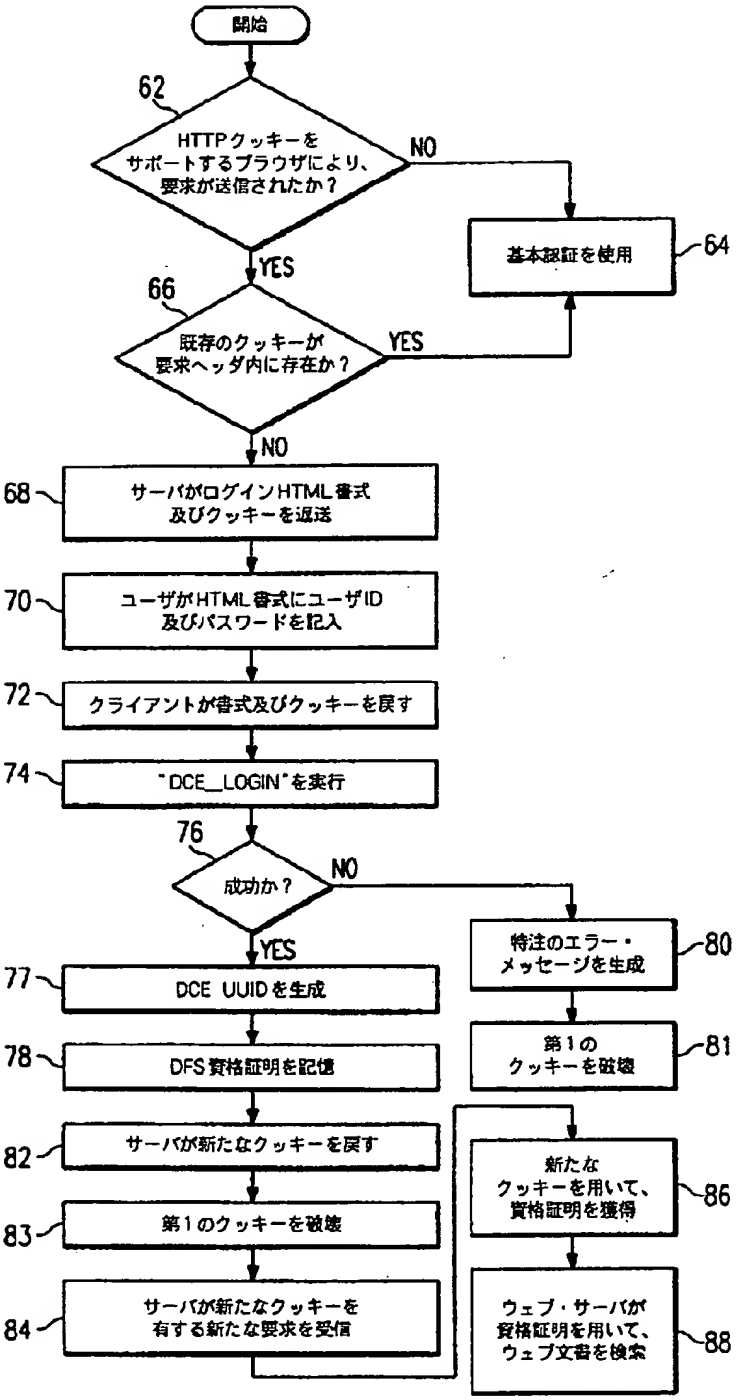
【図2】


30
許可変換
32
ネーム変換
34
経路チェック
36
オブジェクト・タイプ
38
サービス
40
ログ追加
42
エラー

【図3】


10
12
サーバ
クライアント
ブラウザ
16
(a)
(d)
(e)
ウェブ・サーバ
22
(h)
分散
ファイル・
システム
(b,c)
SAFプラグイン
25
50
(f,g)
(i)
27
セッション・マネージャ
29
(f)
アカウント・マネージャ
(j)
52
DCEセキュリティ・サービス
56
58

【図4】


開始
62
HTTPクッキーを
サポートするブラウザにより、
要求が送信されたか？
NO
基本認証を使用
64
YES
66
既存のクッキーが
要求ヘッダ内に存在か？
YES
NO
68
サーバがログインHTML書式
及びクッキーを返送
70
ユーザがHTML書式にユーザID
及びパスワードを記入
72
クライアントが書式及びクッキーを戻す
74
"DCE_LOGIN"を実行
76
成功か？
NO
YES
特注のエラー・
メッセージを生成
80
77
DCE UUIDを生成
78
DFS資格証明を記憶
第1の
クッキーを破壊
81
82
サーバが新たなクッキーを戻す
新たな
クッキーを用いて、
資格証明を獲得
86
83
第1のクッキーを破壊
84
サーバが新たなクッキーを
有する新たな要求を受信
ウェブ・サーバが
資格証明を用いて、
ウェブ文書を検索
88

フロントページの続き

(72)発明者　マイケル・ブラッドフォード・オルト
アメリカ合衆国78729、テキサス州オースティン、ウィストフル・カーブ　12502
(72)発明者　アーンスト・ロバート・プラスマン
アメリカ合衆国78660、テキサス州フルガービル、ドーブ・ハベン・ドライブ　1407
(72)発明者　ブルース・アルランド・リッチ
アメリカ合衆国78681、テキサス州ラウンド・ロック、グレート・オークス・ドライブ　1808
(72)発明者　マッキーラ・アン・ロージレス
アメリカ合衆国78728、テキサス州オースティン、ゴールドフィッシュ・ポンド　14610
(72)発明者　セオドラ・ジャック・ロンドン・シェラダー
アメリカ合衆国78613、テキサス州シダー・パーク、シャディ・ブルック・レーン　1704